Jarosław Zieliński, Sekretarz Stanu Ministerstwo Spraw Wewnętrznych i Administracji 02-591 Warszawa ul. Stefana Batorego 5

Warszawa, 2016-08-05

KANCELARIA PREZESA RADY MINISTRÓW
KANCELARIA SEJMU

BMP-0713-3-103/2016

Odpowiedź na interpelację nr 4777

Odpowiedź Ministra Spraw Wewnętrznych i Administracji na interpelację numer 4777 Posła na Sejm RP Pana Pawła Pudłowskiego w sprawie działań resortu w odniesieniu do cyberprzestępców.

W załączeniu uprzejmie przekazuję odpowiedź Ministra Spraw Wewnętrznych i Administracji na interpelacj interpelację numer 4777 Posła na Sejm RP Pana Pawła Pudłowskiego w sprawie działań resortu w odniesieniu do cyberprzestępców.

Załączniki:

1. ODP. INTERPELACJA 4777.DOC

Dokument został podpisany, aby go zweryfikować należy użyć oprogramowania do weryfikacji podpisu Data złożenia podpisu: 2016-08-17T14:11:06Z

Podpis elektroniczny

Minister
Spraw Wewnętrznych
i Administracji

BMP-0713-3-103/2016/EW

Pan
Marek Kuchciński
Marszałek Sejmu RP

Szanowny Panie Marszałku,

w odpowiedzi na interpelację numer 4777 Posła na Sejm RP Pana Pawła Pudłowskiego w sprawie *działań resortu w odniesieniu do cyberprzestępców* uprzejmie przedstawiam informacje pozostające w zakresie właściwości Ministra Spraw Wewnętrznych i Administracji.

Na wstępie należy wskazać, że pojęcie cyberprzestepczości nie zostało jednoznacznie zdefiniowane na gruncie obowiązujących przepisów prawa. Przyjmuje się, że cyberprzestępczość w szerokim rozumieniu, oznacza wszystkie nielegalne działania popełnione za pomocą systemów albo sieci komputerowych lub ich dotyczące. Natomiast w ścisłym znaczeniu - przestępstwa dokonane za pomocą operacji elektronicznych, wymierzone przeciw bezpieczeństwu systemów komputerowych oraz przetwarzanych przez ww. systemy danych. Dodatkowo pragnę zwrócić uwagę na fakt, że w większości przypadków - poza atakami wymierzonymi w funkcjonowanie systemów teleinformatycznych - cyberprzestrzeń nie stwarza nowego rodzaju przestępstw, a jedynie dostarcza nowych środków lub metod do prowadzenia działalności przestępczej lub stanowi nową przestrzeń, w której taka działalność jest prowadzona.

Należy również wskazać, że przestępstwa określane jako komputerowe nie mają odrębnego przedmiotu ochrony, a w zwalczaniu cyberprzestępczości wykorzystywane są przepisy prawa stosowane do ścigania sprawców innych kategorii przestępstw.

Podstawowym aktem prawnym, w zakresie walki z omówionym zjawiskiem w Polsce, pozostaje ustawa z dnia 6 czerwca 1997 r. *Kodeks karny* (Dz. U. Nr 88, poz. 553 z późn. zm.), która penalizuje m.in. następujące zachowania:

- tworzenie fałszywych tożsamości, fałszywych profili, podszywanie się pod inną osobę (art. 190a § 2 *K.k.*);
- rozpowszechnianie pornografii w sposób narzucający tego rodzaju treści osobom, które sobie tego nie życzą; produkowanie, utrwalanie, sprowadzanie, przechowywanie, posiadanie, rozpowszechnianie, prezentowanie i uzyskiwanie dostępu do treści pedofilskich, związanych z prezentowaniem przemocy i zoofilskich (art. 202 *K.k.*);

ul. Stefana Batorego 5
02-591 Warszawa, Polska
mswia.gov.pl

tel. +48 22 621 20 20
fax +48 22 601 39 88

- propagowanie ustrojów totalitarnych oraz treści rasistowskich i ksenofobicznych oraz wytwarzanie i utrwalanie ww. treści w celu ich rozpowszechniania (art. 256 *K.k.*);
- włamania do systemów komputerowych - *hacking* (art. 267 § 1 *K.k.*);
- nielegalne niszczenie, uszkadzanie, usuwanie, zmienianie zapisu istotnej informacji na nośniku informatycznym albo znaczne utrudnianie lub udaremnianie możliwości zapoznania się z nią (art. 268 § 2 *K.k.*);
- atak na zasoby informatyczne (art. 268a *K.k.*);
- atak na zasoby lub urządzenia informatyczne instytucji państwowych lub samorządowych (art. 269 § 1 i 2 *K.k.*);
- atak na system komputerowy lub sieć teleinformatyczną (art. 269a *K.k.*);
- udostępnianie urządzeń, programów lub danych służący popełnianiu przestępstw (art. 269b *K.k.*);
- oszustwo komputerowe (art. 287 *K.k.*).

Z informacji uzyskanych z Komendy Głównej Policji (KGP) wynika, że przypadki przestępstw charakterystycznych dla cyberprzestępczości, tj. np. włamania do systemów komputerowych i kradzieże danych informatycznych, podsłuchy komputerowe czy ataki na urządzenia sieciowe zgłaszane są Policji sporadycznie. Powyższe wynika przede wszystkim z niskiej świadomości użytkowników sieci telekomunikacyjnych i Internetu, którzy niejednokrotnie nie zdają sobie sprawy, że stali się ofiarą cyberprzestępstwa. Natomiast przedsiębiorcy często zatajają fakt stania się ofiarą tego typu przestępstw ze względów wizerunkowych bądź z obawy przed utratą zaufania klientów. Takie zachowania w znacznym stopniu utrudniają ustalenie rzeczywistej skali opisywanego zjawiska oraz wskazanie – co szczególnie istotne w kontekście wnioskowanych przez Pana Posła danych – liczby ofiar poszczególnych kategorii przestępstw popełnianych z wykorzystaniem sieci komputerowych, w tym odsetka osób, które zgłaszają fakt popełnienia ww. przestępstw.

Niezależnie od powyższego należy wskazać, że Policja gromadzi i przetwarza wszystkie uzyskane informacje i dane statystyczne o cyberprzestępstwach – podobnie jak o innych kategoriach stwierdzonych przestępstw – w Krajowym Systemie Informacyjnym Policji (KSIP). Gromadzone informacje dotyczą wszystkich przypadków naruszeń przepisów karnych, z uwzględnieniem podmiotowych i przedmiotowych cech poszczególnych rodzajów przestępstw.

Z posiadanych informacji wynika, iż w pierwszym półroczu 2016 roku odnotowano 25.824 przestępstwa dokonane przy wykorzystaniu sieci komputerowych, z czego wykryto 17.196 (wykrywalność tej kategorii przestępstw wyniosła zatem 66,6%). W zakresie przestępstw polegających na niszczeniu danych czy żądaniu okupu w pierwszym półroczu 2016 roku w KSIP odnotowano 13 przestępstw z art. 269a *K.k.* (atak na system komputerowy lub sieć teleinformatyczną) oraz 1.265 przestępstw z art. 287 § 1 *K.k.* (oszustwo komputerowe).

W nawiązaniu z kolei do zagadnienia współpracy Policji w zakresie zwalczania cyberprzestępczości ze służbami innych państw uprzejmie informuję, że wymiana informacji odbywa się na bieżąco, przede wszystkim za pośrednictwem Biura Międzynarodowej Współpracy Policji KGP. Jako przykład zrealizowanych działań w omawianym obszarze w 2015 roku warto wymienić m.in. udział Policji w międzynarodowym szkoleniu w ramach NCFTA (National Cyber Forensic and Training Alliance) - konsorcjum skupiającego policje różnych krajów oraz przedstawicieli sektora prywatnego i naukowego czy udział w spotkaniu z funkcjonariuszami BKA (Bundeskriminalamt) dotyczącym aktualnych trendów i zagrożeń w omawianym obszarze. Na uwagę zasługuje również fakt nawiązania współpracy z przedstawicielami komórek do zwalczania cyberprzestępczości analogicznych służb Hiszpanii i Ukrainy.

Ponadto, współpraca międzynarodowa Policji prowadzona jest w ramach Europejskiego Urzędu Policji - Europol. W strukturach Europolu funkcjonuje *European Cybercrime Centre*, którego zadaniem jest m.in. dostarczanie policjom poszczególnych krajów informacji kryminalnej i wywiadowczej czy wsparcie operacji i śledztw prowadzonych w obszarze cyberprzestępczości.

Przechodząc do kolejnego zagadnienia podniesionego w wystąpieniu uprzejmie informuję, że Policja podejmuje działania informacyjne dotyczące bezpieczeństwa w cyberprzestrzeni w ramach prowadzonej profilaktyki społecznej. Wskazane działania mają na celu - co jest szczególnie istotne w kontekście przywołanych wcześniej informacji - zachęcenie osób fizycznych i przedsiębiorców do zgłaszania przypadków cyberprzestępstw. Warto również nadmienić, że podniesienie poziomu ochrony obywateli i przedsiębiorstw w cyberprzestrzeni jest jednym z istotnych aspektów *„Koncepcji działań Policji w zakresie profilaktyki społecznej na lata 2015 - 2018"*.

Jednocześnie wymaga podkreślenia, że działalność informacyjna jest jedynie dodatkową czynnością w ramach przedsięwzięć podejmowanych przez Policję, ukierunkowanych na zwalczanie cyberprzestępczości. Policja jako organ ścigania realizuje bowiem przede wszystkim zadania określone w ustawie z dnia 6 kwietnia 1990 r. *o Policji* (t.j.: Dz. U. z 2015 r., poz. 355 z późn. zm.), do których należą m.in. ochrona życia i zdrowia ludzi oraz mienia przed bezprawnymi zamachami naruszającymi te dobra, ochrona bezpieczeństwa i porządku publicznego, inicjowanie i organizowanie działań mających na celu zapobieganie popełnianiu przestępstw i wykroczeń oraz zjawiskom kryminogennym, a także wykrywanie przestępstw i wykroczeń, w tym również cyberprzestępstw. Wskazane zadania Policja realizuje we współpracy z organami prokuratury.

W kontekście zagadnień podniesionych w wystąpieniu, w szczególności problematyki pomocy udzielanej przedsiębiorcom pokrzywdzonym cyberprzestępczością warto nadmienić, ze celem prowadzonych postępowań, poza oczywistym wykryciem przestępstwa, ustaleniem sprawcy i pociągnięciem go do odpowiedzialności karnej, pozostaje również ochrona interesów pokrzywdzonych (również osób prawnych).

ul. Stefana Batorego 5
02-591 Warszawa, Polska
mswia.gov.pl

tel. +48 22 621 20 20
fax +48 22 601 39 88

Na marginesie warto nadmienić, że w zakresie ochrony pokrzywdzonych przestępczością komputerową szczególną rolę pełni działający w strukturach Agencji Bezpieczeństwa Wewnętrznego Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL.

Przedstawiając powyższe pragnę jednocześnie poinformować, że informacje dotyczące problematyki przestępczości w cyberprzestrzeni opracowane na podstawie danych KGP, a także Agencji Bezpieczeństwa Wewnętrznego, Służby Celnej, Prokuratury Generalnej, Ministerstwa Cyfryzacji oraz Ministerstwa Sprawiedliwości zawiera publikowany corocznie *Raport o stanie bezpieczeństwa w Polsce.* Przedmiotowy dokument dostępny jest na stronie internetowej Biuletynu Informacji Publicznej Ministerstwa Spraw Wewnętrznych i Administracji pod następującym adresem:
https://bip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html

Z poważaniem,

MINISTER

SPRAW WEWNĘTRZNYCH I ADMINISTRACJI

z up. Jarosław Zieliński

Sekretarz Stanu

Otrzymuje:
Sekretariat Prezesa Rady Ministrów w Kancelarii Prezesa Rady Ministrów.

ul. Stefana Batorego 5
02-591 Warszawa, Polska
mswia.gov.pl

tel. +48 22 621 20 20
fax +48 22 601 39 88